TERCERA ETAPA • AÑO 13

jurídica

Martes 28 de enero de 2025

926

SUPLEMENTO DE
ANÁLISIS LEGAL DE
EL PERUANO

HOY, 28 DE ENERO, EL DÍA DE LA PROTECCIÓN DE DATOS RESALTA EL AVANCE DE PAÍSES COMO EL PERÚ HACIA INICIATIVAS INTEGRALES.

Protección de datos: un pilar global

PÁG. 3 RICHARD AGUILAR DÍAZ **PÁGS 4-5** ALEXANDRA EGAS

PÁG. 2 COMPLIANCE EN CADENAS CRÍTICAS DE SUMINISTRO. **DINO CARLOS CARO CORIA**

PÁGS. 6-7 LA FIGURA DEL TRABAJADOR DE CONFIANZA EN LA NORMATIVA DEL PERÚ. **GONZALO COSTA VINDROL**

PÁG. 8 LA IMPORTANCIA DEL OBJETO SOCIAL EN LAS EMPRESAS PERUANAS. **ANA CAROLINA ANDRADE TERÁN**

EL DEBER AMPLIADO EN LA VALORACIÓN DEL RIESGO

Compliance en cadenas críticas de suministro

Esfuerzo se justifica cuando están involucrados riesgos para intereses de alto valor, como la vida, la salud de las personas, los derechos laborales, el medioambiente y otros.

El llamado compliance ad extra hace referencia a lo que está más allá de las relaciones de negocios que tiene la empresa de modo directo o inmediato, implica extender la valoración del riesgo, la debida diligencia más allá del concreto socio de negocios, bien se trate de un cliente o proveedor, e incluso, por extensión, un colaborador. Este deber extendido no es la regla, sino la excepción, rige en situaciones de riesgos especialmente identificados o tasados. Ejercer el compliance más allá del entorno inmediato cuesta más, y ese gasto solo se justifica ante industrias o circunstancias especialmente riesgosas.

Una empresa de maquinarias para el sector minero tiene la obligación de verificar que su cliente no las utilice para la minería ilegal. Un sujeto obligado que trata con una persona expuesta políticamente (PEP), bien como cliente o colaborador, tiene el deber de ejecutar una debida diligencia reforzada que involucra al entorno familiar o personal del PEP. Si una empresa exporta productos agrícolas o textiles que adquiere de terceros, la debida diligencia podría ir más allá del proveedor directo y extenderse a la cadena de suministros de este para descartar cadenas de explotación o esclavitud laboral.

DINO CARLOS
CARO CORIA

CEO EN CARO & ASOCIADOS

El compliance en la cadena de suministros es una forma de compliance ad extra o "más allá de las narices de la empresa". Como describe Ontiveros Alonso, "la implementación de un criminal compliance program ad extra se traducirá en un blindaje jurídico para la organización. Así, esta deberá omitir la vinculación con cualquier otro ente colectivo que esté implicado en la comisión de un delito, mientras que al mismo tiempo se encargará de establecer controles a la cadena de suministro, evitando probables hechos delictivos cometidos por proveedores". Este esfuerzo de compliance se justifica cuando esta cadena involucra riesgos para intereses de alto valor, como la vida, la salud de las personas, los derechos laborales, el medioambiente, etcétera. En estos casos la empresa debe internalizar los costos de esa cadena de prevención, dado el riesgo creado por su pactividad o negocio que le resulta beneficioso.

Es excepcional, también de modo extraordinario, los sistemas legales imponen la debida diligencia en la cadena de suministros. En Europa, por ejemplo, la Modern Slavery Act del 2015 del Reino Unido, la Loi de Vigilance francesa del 2017 y la Lieferkettensorgfaltspflichtengesetz (LkSG) alemana del 2021, obligan a las empresas de alta facturación a extender la debida diligencia cuando la cadena de suministros involucra proveedores extranjeros, a fin de evitar violaciones a los derechos humanos, el trabajo forzado, la esclavitud moderna o daños ambientales. En la Unión Europea (UE) rige la reciente Directiva (UE) 2024/1760 del Parlamento Europeo y del Consejo, adoptada el 13.6.24, sobre diligencia debida de las empresas en materia de sostenibilidad, cuyo objetivo es garantizar que las empresas europeas, y algunas no europeas que operen en el mercado interior, cumplan con altos estándares en derechos humanos y medioambientales

"La prevención en la cadena de provisiones no puede encomendarse únicamente a las empresas".

a lo largo de toda su cadena de suministro, un enfoque que busca reforzar el compromiso de la UE con la protección ambiental y social, alineándose con los principios del Acuerdo de París y las Normas de la OCDE sobre empresas multinacionales.

En Hispanoamérica no existen reglas similares, ni regionales ni locales, tampoco normas que impongan el deber de implementar compliance en derechos humanos, por ejemplo, en el caso de industrias extractivas. La no regulación (hard law) es precisamente el espacio para el compliance, la autorregulación regulada. En el caso del Perú, aunque la ley no prevé de modo expreso que las empresas mineras ejerzan la debida diligencia en toda la cadena de suministros, el riesgo asociado a la minería ilegal y el lavado de activos demandan que los programas de mining compliance si contemplen, como deberes autoimpuestos, esa debida diligencia, como una forma de protegerse a si mismas y hasta de supervivencia corporativa, cuando operan, por ejemplo, en zonas como Pataz, La Libertad, donde la millonaria industria de la minería ilegal gobierna la economía local y no son infrecuentes los casos de negación del Estado, por ejemplo, la destrucción de infraestructura crítica como torres de alta tensión y hasta gravísimas violaciones a los derechos humanos, como el reciente caso de las fosas comunes descubiertas por las autoridades en una zona gobernada por los capos de la minería ilegal.

Estos ejemplos extremos revelan que, como es obvio, la prevención en la cadena de provisiones no puede encomendarse únicamente a las empresas, la ausencia de Estado, la falta de autoridad, la ausencia de las prestaciones públicas más elementales no son responsabilidad del sector privado sino enteramente del Estado. Mientras el crimen organizado conserve ese poder, el compliance en la cadena de suministros es para las empresas una forma de compliance de supervivencia, el único modo de marcar la diferencia entre una industria legal y una empresa criminal.

[1] ONTIVEROS ALONSO, Miguel. "Delincuencia organizada corporativa: su prevención mediante el criminal compliance". En: Matellanes Rodríguez, Nuria. Terrorismo, delincuencia organizada y justicia transicional. Salamanca, USAL 2020, pp. 177-178.

jurídica | DIRECTOR (e): **Félix Alberto Paz Quiroz** | Subdirector: **Omar Swayne Recuenco** | Editora: **María Avalos Cisneros** (mavalos@editoraperu.com.pe)
Coordinador: **Paul Herrera Guerra** | Jefe de Diagramación: **Julio Rivadeneyra Usurín** | Teléfono: **315-0400 (2016)**

Las opiniones vertidas son de exclusiva responsabilidad de los autores. Sugerencias y comentarios: mavalos@editoraperu.com.pe

Jurídica es una publicación de El Peruano
2008 © Todos los derechos reservados

DÍA CONMEMORATIVO DE UN DERECHO EN EVOLUCIÓN

Datos personales en la era digital

Desde 1981, cada 28 de enero, el Día de la Protección de Datos destaca la importancia de promover la armonización de normativas globales para salvaguardar la privacidad frente a retos como la ingteligencia artificial, la ciberseguridad y los derechos digitales.

Cada 28 de enero se conmemora el día de la protección de datos personales a nivel internacional. Tal fecha fue elegida porque, el 28 de enero de 1981, el Consejo de Europa aprobó el primer instrumento jurídicamente vinculante a nivel internacional en materia de protección de datos personales, que fue plasmado en el multicitado "Convenio Nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal".

Hoy en día, a nivel internacional, los países democráticos tienen reconocido e incorporado en sus ordenamientos jurídicos el derecho a la protección de datos personales, si bien, la panoplia normativa en materia de privacidad aún no cuenta con un grado de madurez homogéneo en tales estados, no obstante, también se evidencia la tendencia enfocada hacia la armonización internacional y regional, tanto de la normativa en esta materia como de los criterios para su aplicación, ejemplos destacados de ello son la Global Privacy Assembly (GPA) y la Red Iberoamericana de Protección de Datos (RIPD). Y tales organizaciones cobran un enorme sentido si partimos de la premisa de que la privacidad es un derechos humano y fundamental que precisa contar con un sistema internacionalmente armonizado de protección, a fin de facilitar a los individuos superar el galimatías con el que hoy deben lidiar para poder ejercer sus derechos, que se ven fácilmente conculcados en sede digital. Con mayor razón, si partimos de la base que en el mundo digital no existen fronteras.

RICHARD **AGUILAR DÍAZ**

DIRECTOR DEL ÁREA DE AI LEGAL TECH EN CARO & ASOCIADOS

Recordemos que en el marco de la 88ª sesión plenaria de la Asamblea General de las Naciones Unidas, el citado órgano principal de la ONU, emitió la resolución A/RES/78/287, de fecha 7 de junio del 2024, por la que el 2025 fue declarado "Año Internacional de la Ciencia y la Tecnología Cuánticas". Y lo destacable de la citada resolución es, por todas, la recomendación de toma de conciencia pública sobre la importancia de la ciencia y las aplicaciones cuánticas, junto con el llamamiento a "garantizar que se presta atención a la aplicación de la ciencia y la tecnología cuánticas para el desarrollo sostenible", entendiendo este llamamiento en clave de cumplimiento normativo, humanismo y sostenibilidad.

En lo referido a la tecnología, la coyuntura actual tiene el foco en la inteligencia artificial (IA), léase, IA enjambre, IA cuántica, y, la más popular, IA Large Language Model (LLM), entre otros modelos de IA que van demostrando tanto sus beneficios como desventajas, como son la automatización de procesos, liberación de tareas repetitivas para dedicar a tareas añadiendo valor, frente a los *deepfake,* ciberataques con IA, entre otros, respectivamente.

Llegados a este punto, teniendo en cuenta el estado del arte, conviene mencionar que aún queda camino por recorrer en los puntos clave en materia de protección de datos, como por ejemplo:

Falta de información a la ciudadanía por parte de las administraciones centrales, regionales y locales respecto de cuáles son y cómo se ejercen los derechos a la protección de datos, léase derechos de Acceso, Rectificación, Cancelación (o supresión) y Oposición, también denominados "derechos ARCO". Asimismo, se hace hincapié en que se debe señalar cuál es el canal y la vía accesible a la ciudadanía que facilita el ejercicio de estos derechos.

Derecho al olvido digital, desindexación de datos personales y libertad de información: al respecto, las autoridades de control y algunos tribunales constitucionales, como máximos intérpretes de la norma fundamental, van sentando jurisprudencia dando luz a los criterios que definen los contenidos, límites de cada derecho, ponderándolos ante un caso concreto.

Gestión de la Ciberseguridad y seguridad de la información, teniendo en cuenta que las medidas de seguridad son exigidas por la normativa de protección de datos y que cada día estamos expuestos y somos testigos de los ciberataques perpetrados directamente (hackeo de nuestros dispositivos celulares, computadoras, etcétera), como indirectamente (hackeos a nuestros proveedores de servicios de energía, telefonía, banca, etcétera).

A modo de conclusión, resulta alentador apreciar que existen movimientos internacionales (GPA y RIPD) que sirven de punto de encuentro de legisladores en materia de protección de datos y de las autoridades de control de distintos estados, evidenciándose que están avanzando hacia la armonización tanto de la regulación como de la interpretación y aplicación de la normativa, en clave de seguridad jurídica, tendencia que, en mi opinión, beneficiará tanto a los responsables encargados del tratamiento como a los titulares de los datos personales.

"Hoy en día, a nivel internacional, los países democráticos tienen reconocido e incorporado en sus ordenamientos jurídicos el derecho a la protección de datos personales".

AGENDA CLAVE PARA EL DESARROLLO ECONÓMICO Y LA COMPETITIVIDAD

Protección de datos en el Perú: retos legales

Cada 28 de enero se celebra el Día de la Protección de Datos Personales, recordando la importancia de la privacidad. Hoy, el Perú enfrenta un momento decisivo para consolidar un marco normativo sólido sobre esta materia.

ALEXANDRA **EGAS**

ASOCIADA DE DENTONS PERÚ

Cada 28 de enero, el mundo celebra el Día Internacional de la Protección de Datos Personales, un recordatorio anual de la importancia de resguardar la privacidad en un entorno cada vez más digital. Esta fecha fue instituida por el Consejo de Europa en el 2006, a la firma del Convenio 108, siendo el primer tratado internacional que abordó de manera integral el derecho a la privacidad y la protección de datos personales.

La protección de los datos personales no es un tema menor. En la actualidad, la información que compartimos –desde nuestro nombre hasta datos sensibles como nuestra ubicación, preferencias o imagen– es un activo invaluable para empresas, gobiernos y ciberdelincuentes. La falta de medidas adecuadas para resguardar esta información puede dar lugar a violaciones graves de la privacidad, fraudes y pérdidas económicas. Por ello las normativas en esta materia, como el recientemente actualizado Reglamento de la Ley Nº 29733 de Protección de Datos Personales en el Perú, aprobado por el Decreto Supremo N° 016-2024-JUS, buscan fortalecer las herramientas legales para garantizar que la privacidad sea respetada en todo momento.

Hito para el país

El Perú, al igual que otras naciones, ha reconocido la necesidad de adaptar su marco normativo a los retos de la era digital. A finales de noviembre del 2024 se publicó el nuevo Reglamento de la Ley Nº 29733, que incluye importantes avances, entre ellos la figura del Oficial de Cumplimiento de Datos Personales, un rol similar al Delegado de Protección de Datos europeo.

A partir de noviembre del 2025, y de manera progresiva, las empresas que tratan datos personales en territorio peruano deberán designar a este oficial, quien será el encargado de supervisar el cumplimiento de la normativa, asesorar a los empleados y actuar como punto de contacto con la Autoridad Nacional de Protección de Datos Personales (ANPD). Aunque esta figura refuerza la capacidad de las empresas para garantizar el manejo responsable de la información, también genera interrogantes: ¿están las organizaciones listas para asumir este reto? ¿Contamos con los profesionales capacitados para desempeñar esta tarea?

El Reglamento también incorpora el derecho de portabilidad de los datos personales, como una suerte de extensión del derecho de acceso ya reconocido, que permite a los usuarios solicitar la transmisión de su información personal entre entidades. Esta medida otorga a los ciudadanos un mayor control sobre su información, adaptándose a las demandas actuales de transparencia y eficiencia en el manejo de datos y reconociendo un derecho que el Reglamento General de Protección de Datos Europeo (RGPD) ya reconoce desde hace años.

Medida clave

Otra de las innovaciones del reglamento es la extensión de su alcance a entidades extranjeras que manejan datos personales dentro del Perú, utilizando medios situados en este territorio. Estas organizaciones deberán designar un representante legal en el Perú para interactuar con la ANPD. Este requisito asegura que todas las empresas, sin importar su ubicación, cumplan con los estándares de privacidad locales, lo que fortalece la soberanía digital del país.

El reglamento también establece nuevas directrices para gestionar los incidentes de seguridad. Por ejemplo, cualquier vulneración que afecte los datos personales deberá notificarse a la ANPD en un plazo máximo de 48 horas. Esta disposición busca fomentar la transparencia y garantizar una respuesta ágil ante posibles amenazas a la privacidad de los ciudadanos.

Igualmente se introduce la regulación sobre lo que se debe entender por "nivel adecuado de protección de datos personales" en el marco de una transferencia internacional de los datos, señalado que para determinar el nivel de protección adecuado de un país, la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales emitirá una resolución con el fin de determinar si este cuenta con una protección equiparable a lo dispuesto en la Ley de Protección de Datos Personales y el Reglamento. Esto, si bien suena bien en papel, podría presentar desafíos, pues las empresas dependerán de una respuesta ágil de la autoridad, lo cual no siempre sucede en nuestra realidad práctica.

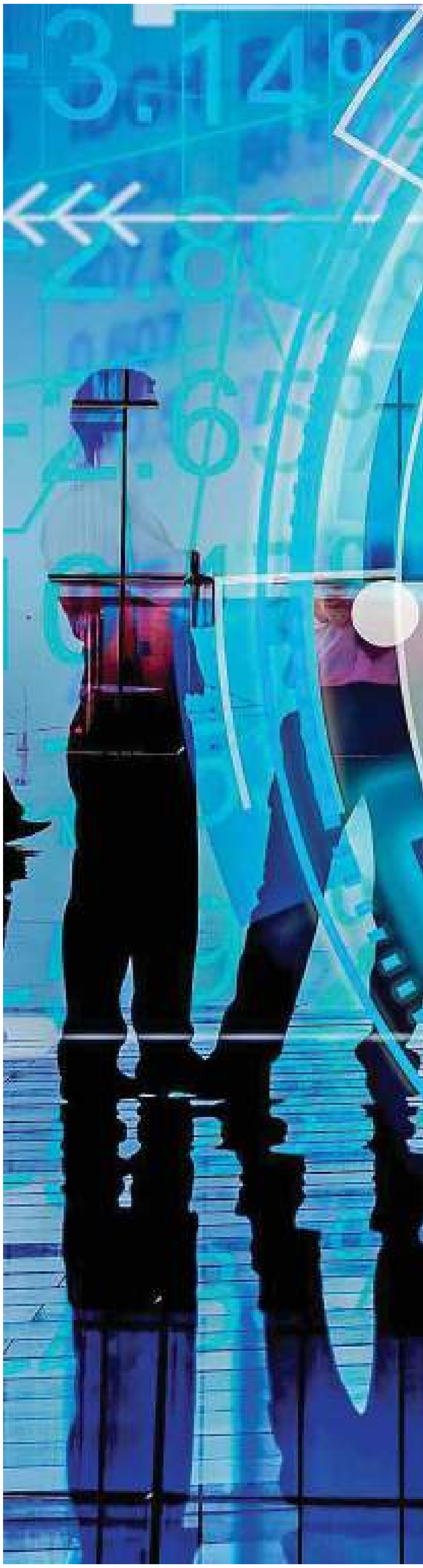
Lecciones y desafíos

El marco europeo es un referente en protección de datos. Entrando en vigor en el 2018, el RGPD transformó la manera en que las empresas manejan la información personal, imponiendo obligaciones estrictas y multas millonarias en caso de incumplimiento. Por ejemplo, la legitimación del procesamiento de datos basada en el interés legítimo o las evaluaciones de impacto obligatorias son áreas donde la normativa peruana aún muestra diferencias significativas.

El nuevo reglamento peruano introduce, además, como recomendación la realización de evaluaciones de impacto en situaciones de alto riesgo, como el tratamiento de datos de menores o la creación de perfiles masivos. Aunque no es una obligación, esta medida se alinea con las mejores prácticas internacionales y refuerza el enfoque preventivo en la gestión de datos personales.

El reglamento peruano incluye otras disposiciones similares, como la designación de un oficial de Cumplimiento de Datos Personales y la notificación de incidentes de seguridad; sin embargo, su implementación práctica podría enfrentar obstáculos debido

"Como profesionales, ciudadanos y organizaciones, es nuestra responsabilidad garantizar que la privacidad continúe siendo un derecho fundamental, adaptándonos a los desafíos de un mundo cada vez más digitalizado".



PERSPECTIVAS A FUTURO

El futuro de la protección de datos en América Latina dependerá de la capacidad de los países para trabajar juntos y establecer estándares comunes que fomenten la interoperabilidad y la confianza en la región. En este contexto, el Perú tiene la oportunidad de liderar, siempre que fortalezca su ANPD, mantenga su participación con miembro de la Red Iberoamericana de Protección de Datos Personales y asegure la implementación efectiva de su ley y nuevo reglamento.
Nuestro país se encuentra en un momento decisivo para consolidar un marco sólido de protección de datos personales. Las disposiciones del nuevo reglamento son un avance significativo, pero su éxito dependerá de una implementación efectiva y de la colaboración entre los sectores público y privado.
El Día Internacional de la Protección de Datos Personales no solo nos invita a reflexionar sobre lo que se ha logrado, sino también sobre el camino que nos queda por recorrer. Como profesionales, ciudadanos y organizaciones, es nuestra responsabilidad garantizar que la privacidad continúe siendo un derecho fundamental, adaptándonos a los desafíos de un mundo cada vez más digitalizado.

a limitaciones en la supervisión y falta de experiencia en el manejo de estos procesos. Esto nos lleva a cuestionar si estamos realmente preparados para cumplir con los estándares que el reglamento propone.

Posición regional

En América Latina, el Perú se encuentra en una posición intermedia en cuanto al desarrollo de su marco normativo de protección de datos. Países como Colombia han liderado el camino con regulaciones más estrictas, como las evaluaciones de impacto obligatorias y altos estándares para transferencias internacionales.

En contraste, Chile aún enfrenta desafíos para consolidar un marco robusto, lo que coloca al Perú en una posición estratégica para liderar en esta área. Con la implementación efectiva del nuevo reglamento, el país tiene la oportunidad de establecerse como un referente regional, siempre que se aborden las limitaciones actuales, como la falta de recursos de la ANPD y la baja cultura de cumplimiento.

Con la publicación del nuevo reglamento nuestro país está haciendo el esfuerzo de reconocer la realidad, un entorne altamente digital y globalizado, pero es importante que no solo existan regulaciones al respecto si no que los privados logren entender estas normativas y que no sea excesivamente costoso implementarlas. La cultura de cumplimiento: un reto urgente.

Uno de los mayores desafíos que enfrenta el Perú es la necesidad de fomentar una cultura de cumplimiento en las empresas y en la ciudadanía. Muchas organizaciones aún perciben la protección de datos como un requisito burocrático en lugar de una oportunidad para construir confianza con sus clientes.

Es importante tener en cuenta que la privacidad de los datos no es solo un derecho, sino una ventaja competitiva. Las empresas que adopten estas normativas de manera proactiva estarán mejor posicionadas para competir en mercados internacionales y responder a las expectativas de sus clientes en términos de transparencia y responsabilidad.

Preparativos

Precisamente para las empresas, la transición hacia este nuevo marco normativo no debe esperar. Es prioritario invertir en formación especializada para designar oficiales de Cumplimiento de Datos Personales capacitados y actualizar las políticas de privacidad. Asimismo, será necesario realizar auditorías internas para identificar brechas en el manejo de datos y establecer protocolos sólidos para prevenir incidentes de seguridad.

Desde el sector público, la ANPD tiene una función crucial que desempeñar. Emitir guías claras, promover capacitaciones y fortalecer sus capacidades de supervisión son pasos indispensables para asegurar que la normativa tenga un impacto real y positivo.

Impacto económico

Un marco normativo sólido no solo protege los derechos fundamentales, sino que también impulsa el desarrollo económico. La confianza en el manejo de datos personales es un pilar esencial para el crecimiento del comercio electrónico, la banca digital y otros sectores emergentes en la era digital.

Al garantizar la privacidad de los datos, el Perú puede atraer inversiones extranjeras y promover la innovación tecnológica, posicionándose como un actor relevante en la economía digital global.

Implementación

El nuevo Reglamento de la Ley Nº 29733 entrará en vigencia el 30 de marzo del 2025, con plazos progresivos para la designación del oficial de Cumplimiento de Datos Personales según el tamaño de las empresas. Las grandes empresas (ventas mayores a 2,300 UIT) tendrán un año para cumplir, mientras que las medianas (1,700 a 2,300 UIT), pequeñas (150 a 1,700 UIT) y microempresas (hasta 150 UIT) dispondrán de dos, tres y cuatro años, respectivamente. Asimismo, la disposición sobre portabilidad de datos será efectiva seis meses después de la entrada en vigor del reglamento, facilitando la adaptación al nuevo marco normativo.

¿QUÉ HAY DETRÁS DE ESTA FIGURA EN EL PAÍS?

Puestos de confianza: riesgos legales y protección laboral

Es necesario un equilibrio en su tratamiento, con una normativa clara y una gestión ética por ambas partes de la relación laboral, para garantizar vínculos laborales justos y equitativos.

GONZALO **COSTA VINDROLA**

SOCIO DEL ÁREA LABORAL DE COSTA, OLIVARES & PALOMINO | ABOGADOS.

La designación de puestos de confianza y de dirección son figuras legales importantes en el mundo laboral, ya que permite mantener una estructura ordenada y jerarquizada de la organización. Sin embargo, ¿qué pasa cuando esta figura se usa de manera incorrecta? ¿Cómo afecta esto a los trabajadores?

Las designaciones de los puestos de confianza y de dirección revisten de particular importancia por las responsabilidades, toma de decisiones y la confidencialidad en la información que estos implican. Sin embargo, el uso indebido de esta figura puede derivar en perjuicios significativos para los trabajadores, vulnerando su derecho a la estabilidad laboral y generando situaciones de inequidad en las relaciones laborales. Este artículo explora la normativa vigente, las implicancias legales y los problemas asociados al abuso de la designación de "confianza" en el Perú.

El marco normativo respecto a la conceptualización de lo que se debe entender como trabajador de confianza y de dirección lo encontramos en el artículo 43° del Decreto Supremo Nº 003-97-TR, en que se considera personal de dirección a aquel que ejerce la representación general del empleador frente a otros trabajadores o terceros, o que lo sustituye compartiendo funciones de administración y control, conceptualizando a su vez al trabajador de confianza como aquel que labora en contacto directo con el empleador o con el personal de dirección, teniendo acceso a secretos industriales, comerciales o profesionales, y, en general, a información de carácter reservado.

Vemos además que los artículos 59° a 61° del Decreto Supremo N° 001-96-TR establecen el procedimiento que se debe seguir para la designación de un puesto como de confianza o dirección (identificación de puestos, comunicación al trabajador y registro en la planilla de pagos); sin embargo, se establece también que el incumplimiento de esta formalidad no acarrea la nulidad en la designación si del análisis de las funciones se verifica que efectivamente el puesto seleccionado realiza funciones propias de un puesto de confianza o dirección, agregándose que el trabajador cuenta con un plazo de treinta (30) días naturales para cuestionar esta calificación, lo que en la práctica judicial no se viene aplicando.

Relación estrecha

Así, observamos que los cargos de confianza y dirección se encuentran estrechamente relacionados entre sí, existiendo el factor de "confianza" en ambos puestos, presentando a su vez, diferencias claras; siendo la principal, el hecho de que el personal de dirección posee poder de decisión y actúa en representación del empleador, con facultades propias de este. En contraste, el personal de confianza colabora estrechamente con el empleador o con el personal de dirección, accediendo a información confidencial y contribuyendo a la toma de decisiones sin tener poder decisorio propio, es justamente esta diferenciación jerárquica la que influye además en la extensión del período de prueba, ya que, si para un trabajador ordinario tenemos que el período de prueba es de tres (3) meses, observamos que para el personal de confianza este periodo se puede extender hasta el tope de seis (6) meses, y en el caso del personal de dirección, el período de prueba puede durar hasta doce (12) meses; obedeciendo estos periodos a la necesidad de evaluar con mayor rigurosidad la adaptación del personal de confianza y dirección en los puestos asignados y el desempeño del mismo.

Otro aspecto por tener en cuenta es que en el 2016 se emitió la sentencia correspondiente a la Casación Laboral Nº 18450-2015-Lima, así como las conclusiones del Quinto Pleno Jurisdiccional Supremo en materia laboral y previsional, en que se consolidó la figura de "retiro de confianza" como causal subjetiva de terminación del vínculo laboral sin derecho a la reposición. Ni al pago de la correspondiente indemnización por despido arbitrario, en caso de estar frente a trabajadores que ingresaron directamente a un cargo de confianza y con la opción de retorno al puesto ordinario anterior o pago de indemnización por despido arbitrario en caso de que el trabajador decida no retornar al puesto ordinario anterior, o en caso de que el empleador se niegue a su retorno, sin que en este último caso exista la opción de solicitar la reposición en sede judicial, lo que generó un incremento, en las designaciones de confianza, como figura alternativa de desvinculación sin opción de reposición.

Ahora, independientemente de que un puesto cumpla o no con los requisitos para ser considerado de confianza o dirección, se observa que en la realidad algunas empresas ven atractiva esta figura por los beneficios que podrían obtener con esta designación, ya que, adicionalmente a la flexibilidad en la forma de terminación del vínculo laboral sin opción de reposición futura, vemos, por ejemplo, que la Ley de Relaciones Colectivas de Trabajo restringe la libertad de afiliación de este grupo de trabajadores (los cuales podrán afiliarse siempre y cuando el estatuto del sindicato respectivo fije que en efecto este grupo de trabajadores se puede afiliar), supeditándose así la libertad sindical de estos trabajadores a la voluntariedad del sindicato, de igual forma, podría generar supuestos de no reconocimiento de indemnización vacacional, en la figura de que se trataría de personal que adoptó el no goce de su descanso vacacional en su oportunidad.

Casos emblemáticos

Dejando la teoría y pasando a la práctica, podemos traer a comentario un caso emblemático: la Casación Laboral Nº 18450-2015-Lima, en que la Corte Suprema de Justicia determinó que solo los trabajadores de confianza promovidos tienen derecho a una indemnización por despido arbitrario, no así aquellos que accedieron directamente al cargo de confianza. Este fallo evidenció la necesidad de una mayor claridad en la normativa para evitar interpretaciones que perjudiquen al trabajador. Añadido a este, otro caso relevante ocurrió en el 2019, cuando un grupo de trabajadores de una empresa minera denunció que fueron designados como de confianza únicamente para evitar su participación en una huelga convocada de manera le-

PREVENCIÓN ANTE EL ABUSO

El empleador también debe buscar métodos de prevención de abusos por parte del trabajador. En este caso, para evitar estos abusos las empresas deben, entre otros:, (i) definir claramente las funciones del puesto, esto es, establecer límites y responsabilidades precisos, (ii) deben implementar controles internos y supervisar el manejo de la información confidencial, (iii) establecer cláusulas de confidencialidad y no competencia para proteger los intereses de la empresa así como (iv) fomentar la ética laboral y crear una cultura organizacional basada en valores.

La figura del trabajador de confianza es fundamental en el ámbito laboral peruano, pero su uso indebido puede generar problemas, tanto para empleadores, como para empleados. Por un lado, algunos empleadores la utilizan como una herramienta para facilitar despidos o limitar derechos laborales. Por otro lado, ciertos trabajadores pueden aprovecharse de su posición para obtener beneficios personales. Es necesario un equilibrio en el tratamiento de esta figura, con una normativa clara y una gestión ética por ambas partes, para garantizar relaciones laborales justas y equitativas.

gal. Posteriormente, la autoridad laboral determinó que estas designaciones eran inválidas, ordenando la restitución de sus derechos sindicales.

Es entonces que, para algunos empleadores, calificar a un trabajador como de confianza o dirección podría ser un mecanismo para precarizar la estabilidad laboral. Citando otro ejemplo, una empresa textil de Lima utilizó esta estrategia para despedir a más de 20 trabajadores, ahorrando costos significativos en indemnizaciones. Es entonces que la designación como trabajador de confianza puede ser utilizada como una herramienta de control, asegurando que el trabajador no tenga la posibilidad de afiliarse a un sindicato o de reclamar ciertos derechos laborales. Este tipo de prácticas son recurrentes en los sectores comercio y construcción. Por ello, al clasificar al trabajador como de confianza, el empleador obtiene mayor libertad para modificar unilateralmente las condiciones laborales, con el argumento de necesidades organizacionales.

La figura del trabajador de confianza es fundamental en el ámbito laboral peruano, pero su uso indebido puede generar problemas, tanto para los empleadores como paralos empleados.

Recomendaciones

El cargo de confianza debe ser utilizado para el fin por el cual fue creado. Algunas recomendaciones para prevenir el uso indebido de esta figura son: el establecer de manera precisa las funciones y responsabilidades que justifican la designación de un trabajador como de confianza, asegurando que cumpla con los criterios legales establecidos. Esto debe estar debidamente registrado en el contrato laboral, y ser aprobado por el trabajador. En segundo lugar, los empleadores deben informar al trabajador, desde el inicio de la relación laboral, sobre la naturaleza de su puesto y las implicancias legales de ser considerado personal de confianza, la transparencia reduce conflictos futuros.

Por parte de las autoridades laborales, estas deben vigilar y sancionar prácticas indebidas relacionadas con la designación de trabajadores de confianza, garantizando el cumplimiento de la normativa vigente, esto es que las inspecciones laborales deben incluir una revisión de los criterios utilizados para esta designación. Aunado a ello, es importante que tanto trabajadores como empleadores conozcan sus derechos y obligaciones respecto a la figura del trabajador de confianza, por lo que las autoridades laborales deben promover relaciones laborales justas y equitativas, para ello se deben fomentar talleres y campañas informativas, los cuales pueden ser herramientas útiles en este sentido.

Aunque los abusos de los empleadores son más frecuentes, también existen casos en que los trabajadores de confianza intentan aprovecharse de su posición, por ejemplo, usando el acceso a la información sensible para beneficio personal, o para renunciar y usar esa información en una empresa competidora o en un negocio propio. Otro caso se daría cuando realmente el trabajador goza de confianza y busca exigir aumentos salariales o beneficios adicionales, argumentando que su función es clave para la empresa y amenazando con desvincularse estratégicamente para presionar al empleador. O también, el trabajador de confianza podría asumir que su permanencia en el puesto es seguro, debido a la relación cercana con el empleador, y, por consiguiente, de manera intencional busca reducir su productividad.

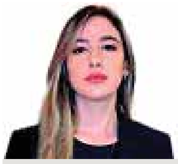
Importante también destacar que un trabajador de confianza podría tomar decisiones que beneficien más sus intereses personales que los de la empresa, como favorecer a familiares en contrataciones o usar recursos para fines personales.

ELEMENTO IDISPENSABLE PARA LAS ORGANIZACIONES

El objeto social como base de las sociedades

Los socios fundadores deben definir el objeto social, que debe ser lícito, claro y preciso, para cumplir con la normativa y evitar controversias, explica la autora.

El objeto social en el ámbito del derecho corporativo constituye un elemento indispensable para la constitución de una empresa, puesto que determina las actividades que la persona jurídica desarrollará en el mercado. De esta manera, al momento de constituir una sociedad, los socios fundadores son los encargados de definir las actividades del objeto social las cuales deben cumplir con requisitos indispensables, estos requisitos consisten en establecer actividades lícitas, determinables, claras y precisas.



ANA CAROLINA **ANDRADE TERÁN**

ASOCIADA JÚNIOR DEL ESTUDIO RODRIGUEZ ABOGADOS & ASOCIADOS

Siendo así, en nuestra legislación peruana, el objeto social se encuentra regulado por la Ley General de Sociedades (Ley N° 26887), específicamente en el artículo 11, en el cual establece que la sociedad circunscribe sus actividades a aquellos negocios u operaciones lícitos que forman parte del contenido del objeto social. De la misma manera, se entienden incluidos en el objeto social los actos relacionados con el mismo que coadyuven a la realización de sus fines, a pesar de no encontrarse expresamente indicados en el pacto social o en el estatuto.

Además, en el artículo 11 de la Ley General de Sociedades (Ley N° 26887) establece que la sociedad no puede tener por objeto desarrollar actividades que la ley atribuye con carácter exclusivo a otras entidades, al respecto, existen casos específicos en los que las actividades que desarrollará una empresa requiere de la autorización de la Superintendencia de Banca y Seguros, estas actividades se encuentran estipuladas en el artículo 11 de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros (Ley Nº 26702).

Es preciso mencionar, que de acuerdo con el artículo 26 del Reglamento del Registro de Sociedades aprobado por la Sunarp mediante Resolución Nº 200-2001-SUNARP/SN, se establece que el objeto social de una empresa no podrá contener expresiones genéricas o ambiguas.

Los socios fundadores son los encargados de definir las actividades del objeto social, las cuales deben cumplir con requisitos indispensables.

Por otro lado, con relación a la obligatoriedad de determinación del objeto social para la constitución de una empresa, esta se fundamenta en la protección que brinda a los socios, asimismo, brinda protección a la sociedad, por último, pero no por ello menos importante, brinda protección a los terceros que contratan con la sociedad.

En la misma línea, la obligatoriedad del objeto social constituye un elemento importante para tomar algunas decisiones, la principal decisión está relacionada con los socios, puesto que, de ello depende la decisión de participar en la sociedad, aportar capital, así como aceptar el riesgo que asumirán los socios al invertir en el negocio. Sin embargo, existen otras decisiones importantes que dependen del análisis del objeto social, entre estas decisiones se encuentra la determinación del nivel de endeudamiento de la sociedad, así como el nombramiento de los primeros administradores.

Por otra parte, debo indicar que cuando una sociedad no ha realizado su objeto social; es decir, no realiza su fin social durante un período determinado o cuando presenta la imposibilidad de realizarlo, conforme lo establece el inciso 2 del artículo 407 de la Ley General de Sociedades (Ley N° 26887), esta situación constituye una causal de disolución de la sociedad.

Es menester señalar que algunos juristas consideran que el objeto social de una sociedad puede estar integrado por más de una actividad económica, operación o negocio, por ello no existe una restricción para que una sociedad integre algunas actividades, es decir, incluir múltiples actividades en el objeto social es una característica en la legislación peruana.

Finalmente, existe un gran sector de la doctrina que está a favor de la aplicación actos ultra vires, los cuales se configuran cuando los administradores de la sociedad sobrepasan lo establecido en el objeto social de una empresa, vulnerando el estatuto de la empresa, lo cual implica además que estos actos adolecen de nulidad absoluta. Ante esta situación, la empresa no asume la responsabilidad por los efectos que derivan del acto nulo. En consecuencia, en los acuerdos societarios que contengan actos ultra vires podrá aplicarse acciones de nulidad, conforme se estipula en la Ley General de Sociedades (Ley N° 26887).